dharma
Merchant Services

iSpyFraud Merchant Use Cases

Use Case One: **Restrict Transactions from Outside of Your Country**

Merchants can use iSpyFraud to restrict transactions outside their own country in two ways:

1. **User Ban>>Geographical Information>>Verify Country**
    a. Using the Verify Country option, merchants can select to *only* look at the customer's billing/shipping addresses. This would prevent any transaction with a billing or shipping address outside the merchant's country from being processed (merchant can choose to either ban or flag for review)
    b. To ban/flag all countries other than their own, the merchant would simply highlight all countries except their own from the list in the Geographical Information section of the User Ban tab, then click "Add".
2. **User Ban>>Geographical Information>>Verify IP Addresses**
    a. If a merchant chooses to verify IP addresses in addition to billing/shipping addresses, iSpyFraud will also weed out transactions where the IP Address is physically located in the banned/flagged country.
    b. This option can only be selected *in addition to* the Verify Country option. Using both together is the safest method of screening for location by country, as a fraudster's physical location often does not match the submitted billing/shipping address.

Example 1: If a merchant sells supplements but doesn't ship internationally due to regulatory laws, that merchant would most likely want to only verify a customer's country by billing/shipping address, rather than IP address, since the restriction they are most concerned with deals with where the merchandise goes, not necessarily where the transaction originates from. Although this provision isn't necessarily a case of fraud, this type of setting could help prevent chargebacks.

Example 2: If a merchant is a non-profit organization that accepts donations from locals, they would most likely select Verify Country *and* IP Addresses. This will ensure that they are screening for users by physical location, rather than the location of the credit card owner—this is especially important in the case of entities that accept donations, as non-profits are commonly targeted by card-testing scams.

Use Case Two: **Protect Yourself from Card-Spinning/Card-Testing Fraud on your ecommerce website**

Card spinning, sometimes called card testing or simply carding, can be spotted in a number of different ways, including:

1. Many authorization attempts in a very short period of time
    a. If a merchant notices an unusually high amount of authorization attempts in a short amount of time, immediate evaluation of those transactions is warranted to assess whether or not fraud is occurring. The merchant should also consider contacting our support team to assist in a thorough evaluation.
2. The first six digits of the card (BIN) for multiple transactions are the same or similar
    a. In this case, a merchant can go to **User Ban>>Credit Cards** and enter the suspicious BIN, followed by a "*" (e.g. "411111*) and select whether to ban or flag that particular user.

3. The transaction amounts are very low ($.01 to $1.00)
    a. Typically, fraudsters who spin cards will first attempt a transaction for a very low amount, just to see if they can get an approval. To help screen this type of testing, a merchant can set a threshold that bans/flags transactions under a certain amount (such as $1.00). This might not be possible for certain merchants, as they might have legitimate transactions for amounts that low.
4. A spike in declined transactions in a merchant's reporting
    a. If a merchant notices an unusual amount of declined transactions, the best course of action may be to contact support to get help assessing whether or not there's fraud involved, and where it might be coming from.
5. Nonsensical names and/or emails, or the same name/email for multiple transactions in a short amount of time
    a. When something like this happens, a merchant can block the user(s) by selecting **User Ban>>Email Address** and enter the email(s) corresponding with the fraudulent transactions. If the merchant notices that all of the fraudulent transactions are coming from the same domain, the merchant can screen all emails from a specific domain by entering "*@emailaddress.com".

Use Case Three: **Protect Yourself from Employee Fraud**

Depending on the type of employee fraud and/or credit card abuse the merchant is experiencing, various actions can be taken.

1. If employees are entering amounts that are either higher or lower than the merchant's business requires, a minimum and/or maximum amount threshold can be implemented.
    a. To set a minimum amount threshold, go to **Thresholds>>If single transaction amount is less than $[desired amount]**, enter the amount you want to screen for, choose the action you wish to take (Flag for Review or Deny Transaction), and click "Update".
    b. To set a maximum amount threshold, go to **Thresholds>>If single transaction amount exceeds $[desired amount]**, enter the amount you want to screen for, choose the action you wish to take (Flag for Review or Deny Transaction), and click "Update".
2. If the card abuse is related to multiple transactions, or if a merchant's business model dictates that a customer's credit card should only be processed once in a given timeframe (e.g. in the case of a monthly subscription-based business), the merchant can set a credit card threshold to screen for inappropriate usage.
    a. To set a credit card threshold for daily use, go to **Thresholds>>If daily attempted transaction count for CC exceeds [desired amount]**, enter the amount you wish to screen for, choose the action you wish to take (Flag for Review or Deny Transaction), and click "Update"
        i. The same process can be done for weekly, monthly, and yearly transaction counts.

Use Case Four: **You Have Multiple MIDs but Don't Want Your Transactions Scrubbed on Every MID**

iSpyFraud can be used for an entire gateway account, or be customized to only screen the transactions run under a specific MID. In addition, iSpyFraud can also be customized so that any global rules are ignored on a per-processor basis.

When it comes to setting different rules for different MIDs, this can be accomplished in one of two ways. A merchant can either set global rules and then single out specific MIDs to have them bypassed by those rules, or set entirely different rules for different MIDs.

1. To start, merchants must have at least two active MIDs boarded on their gateway account, and must be logged in as a user with permissions to all processors.
    a. When clicking through iSpyFraud tabs **Thresholds, User Ban,** or **Exceptions**, the merchant will see a subtab labeled **All Processors**, then a subtab for each active MID on their account.
        i. If there are rules that the merchant wants to apply to all MIDs, those rules should be set in the **All Processors** tab.
        ii. Any rules that the merchant wants to apply specifically to a certain MID should be set under that MID's subtab.
        iii. If there are no global rules and every rule is specific to a certain MID, the merchant should not customize the **All Processors** tab, and instead set all rules within each MID's subtab.

Use Case Five: **You Process Recurring Transactions and Don't Want to Accept Pre-Paid Cards**

Prepaid cards have their uses, but when it comes to recurring transactions, some merchants may be wary of accepting prepaid cards, as there is a chance that money will run out before the timeframe for the recurring transactions expires.

1. To prevent the use of prepaid cards, the merchant can reach out to the Card Associations to obtain a list of BINs associated with a prepaid cards and enter them under **User Ban>>Credit Cards**.
    a. If there are multiple BINs, the merchant can load up to 5000 entries at once into **User Ban>>Batch Ban** by selecting the **Credit Card/Bank** radio button.
2. The merchant can also block *all* cards except for specific BINs by going to **User Ban>>Credit Cards** and ban/flag cards beginning with the first number associated with certain card brands (e.g. entering "4*" would block all Visa cards).
    a. Once the desired card brands are blocked, the merchant can go to **Exceptions>>Credit Card White List** and add any card numbers/BINs that the merchant wants to accept.
    b. For multiple acceptable card numbers/BINs, the merchant can go to **Exceptions>>Batch White List** and select the **Credit Card/Bank** radio button, then upload a list of acceptable cards.